AMENDMENTS TO THE CLAIMS:

This listing of claims will replace all prior versions, and listings, of claims in the application:

LISTING OF CLAIMS:

1. - 15. (Canceled)

16. (Previously Presented) A method of securing access to a piece of equipment, the method comprising:

obtaining a reference datum for an authorized user, wherein said reference datum comprises at least an authentic biometric signature;

storing an encrypted version of said authentic biometric signature on said piece of equipment;

acquiring, at a sensor, a plain biometric signature for a user requesting access to said piece of equipment;

transmitting, from said piece of equipment, said encrypted biometric signature to an authentication medium that is separate from said piece of equipment;

decrypting, in said authentication medium, said encrypted authentic biometric signature received from said piece of equipment;

verifying, in said authentication medium, the authenticity of said plain biometric signature by comparing said plain biometric signature of said user with said decrypted authentic biometric signature of an authorized user; and

granting said user access to said piece of equipment if said comparison is successful and denying access if said comparison fails.

17. (Previously Presented) The method according to claim 16, wherein said authentication medium is an electronic card.

18. (Previously Presented) The method according to claim 17, wherein said electronic card includes a decryption module.

19. (Previously Presented) The method according to claim 17, wherein said electronic card includes a comparison module, and said comparing is performed in said electronic card.

20. (Previously Presented) The method according to claim 17, wherein said electronic card further comprises an encryption module, and transmits said encrypted authentic biometric signature to said piece of equipment for storage thereon.

21. (Previously Presented) A method of securing access to a piece of equipment, the method comprising:

creating a reference datum for an authorized user in an authentication medium separate from said piece of equipment, wherein the creation of said reference datum comprises:

(i) inputting a personal identification code for said authorized user on a keyboard;

(ii) detecting, at a sensor, a plain authentic biometric signature for said authorized user;

(iii) encrypting said plain authentic biometric signature by means of a private key;

(iv) sending said encrypted authentic biometric signature said piece of equipment;

(v) associating said personal identification code with said encrypted authentic biometric signature; and

(vi) storing said encrypted authentic biometric signature and said associated personal identification code on said piece of equipment;

receiving a personal identification code inputted on a keyboard;

acquiring, at a sensor, a plain biometric signature of a user requesting access to said piece of equipment; and

verifying the authenticity of said plain biometric signature for a user requesting access to said piece of equipment, wherein said verifying comprises:

(i) matching said personal identification code with an encrypted authentic biometric signature stored on said piece of equipment;

(ii) sending said encrypted authentic biometric signature, that is associated with said personal identification code, from said piece of equipment to said authentication medium;

(iii) decrypting said authentic biometric signature, on said authentication medium, by means of the private key;

(iv) comparing, on said authentication medium, said decrypted authentic biometric signature with said plain biometric signature of said user requesting access to said piece of equipment, to provide a comparison result; and

(v) granting access to said user requesting access to said piece of equipment if said comparison result is successful and denying access if said comparison result fails.

22. (Previously Presented) The method according to claim 21, wherein said authentication medium is an electronic card.

23. (Previously Presented) The method according to claim 22, wherein said electronic card includes a decryption module.

24. (Previously Presented) The method according to claim 22, wherein said electronic card includes a comparison module, and said comparing step is performed in said electronic card.

25. (Previously Presented) The method according to claim 22, wherein said electronic card includes an encryption module, and transmits said encrypted authentic biometric signature to said piece of equipment for storage.

26. (Previously Presented) A system for securing access to a piece of equipment, comprising:

a storage device in said piece of equipment, for storing an encrypted authentic biometric signature and a corresponding personal identification code of an authorized user;

a sensor for acquiring a plain biometric signature of a user requesting access to said piece of equipment; and

an authentication medium separate from said piece of equipment and having a controller, wherein said controller:

receives said encrypted authentic biometric signature, associated with said personal identification code, from said storage device in said piece of equipment;

decrypts said authentic biometric signature by means of a secret key;

compares said decrypted authentic biometric signature with said plain biometric signature of said user requesting access to said piece of equipment, to provide a comparison result; and

grants access to said user requesting access to said piece of equipment if said comparison is successful and denying access if said comparison fails.

27. (Previously Presented) The system according to claim 26, wherein:

said storage device includes at least one computer for storing a plurality of encrypted authentic biometric signatures and a corresponding plurality of personal identification codes for a corresponding plurality of authorized users, wherein said at least one computer:

delivers an encrypted authentic biometric signature associated with a personal identification code to said authentication medium when receiving an access request from a user, such that said authentication medium is capable of providing a plurality of users secure access to said piece of equipment.

28. (Previously Presented) The system according to claim 26, wherein said authentication medium is an electronic card having a memory storing a secret key that cannot be read from outside.

29. (Previously Presented) The system according to claim 27, further comprising an encryption module that encrypts an authentic biometric signature supplied in plain form to said sensor and delivers said encrypted authentic biometric signature for storage in said piece of equipment, in response to an encryption command.

30. (Previously Presented) The system according to claim 29, wherein said secret key is a private key having a matching public key, and wherein said encryption module is included in said at least one computer and uses said matching public key to encrypt authentic biometric signatures.

31. (Currently Amended) The method according to claim 16, wherein said piece of equipment includes an encryption module for encrypting ~~an~~ the authentic biometric signature for storage in said piece of equipment.